OSG Security

Mine Altunay

09/25/2007

OSG Vision and Goals (Security for FY08)

- Complete the work on VO-Site collaboration
  - Authentication and authorization
    - Today there is an incomplete link between a VO and a Site. (manual communication of VO policy definition to site policy enforcement.)
    - Need to provide seamless interaction.
    - Must get rid of manual intervention.
  - Forward thinking: what this work lead to in FY09 and FY10:
    - Automated trust life-cycle.
    - Fine grained privileges that are delegated (ie have limited proxies passing through the system).

Current OSG Work

- Building the policy work to accomplish and complete the VO Site collaboration:
  - VO security Policy, Site Security Policy, contracts, service agreements, etc…expect to have first complete pass in place by the end of 2007.
- Soon will need the tools to realize the policies
  - Will need development. These tools do not exist today. Who , what , when ? See next slide

OSG expectations

- VO - Site collaboration : Authentication:
  - Issue and distribute certs for VOMS/VOMRS and VO Representatives (side Q: who represents a VO in a collaboration?)→ comes from the current VO Services (privilege) project.
  - VO & Sites must mutually authenticate to collaborate (trust?) → Comes from the current/future VO services project ?
  - Must sign the collaboration agreement → not yet in place, VO services project
  - By-product: Need to get rid of VOMS/GUMS synch because certs are distributed → expect this from VO services project

OSG Expectations

- VO Site Collaboration: Authorization/Privileges:
  - Define job contracts (priorities, execution env, storage capacity, etc) → should this really be under authz, can it move to another activity? If so what, who when ? How to communicate these end-end ?
  - Define and enforce agreed upon privileges both by the VO and Site: Semantic tools for defining agreed privileges + enforcement of the privileges → can deliverable from Tech X SBIR be used to a reasonable schedule ? Could/should FNAL put in additional effort here?
  - Which privileges are needed for which job → fine grained access
    - Dcache + Storage . Do we need a different access control model for storage? → part of consulting and discussions of VO services project?

Which privileges are needed for which job, → fine grained access cont..

- The least privilege principle? **Privacy** of the attributes proxies → should privacy be a separate bullet point with separate controls?
- if proxies (attributes) travel between sites, privacy of the attributes → gLExec, expanded end-end security, new project ? Where does Epensys fit here?
- Speaking of privacy: account mapping in GUMS, why do we need all VO members downloaded in GUMS? Probably not. Getting rid of VOMS/GUMS synch, will solve this partially → expect this from the VO services project.

– Monitoring

- Provide monitoring for VO/Site contracts. Who, what, when? → no one yet signed up to deliver this.